(Unclassified)

NAVAL WAR COLLEGE

Newport, R.I.

APPLYING OPERATIONAL ART TO ASYMMETRICAL THREATS WITHIN UNITED STATES

by

Jon M. Sweet
GS-13, Space and Naval Warfare Systems Command

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: Jon Sweet

13 February 1998

Colonel Mackubin T. Owens
USMCR (Retired)
Faculty Advisor

13 Feb 98
Date

Paper directed by:
Captain Mike Tollefson, USN
Lieutenant Colonel Mike Norton, USA

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Applying Operational Art To Asymmetrical Threats Within United States (Unclassified)	
9. Personal Authors: Mr. Jon M. Sweet, Space and Naval Warfare SYSCOM	
10.Type of Report: FINAL	**11. Date of Report:** 13 February 1998
12.Page Count: 25	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Operational Art, Asymmetrical Warfare, Posse Comitatus, Interagency, Domestic Crisis Response, Critical Infrastructure.	

15.Abstract: The United States position of military dominance has continually evolved since World War II. While many factors are responsible for this elite status, perhaps the most important is the careful consideration given to jointness and operational effectiveness. Given the Unites States' seemingly overwhelming conventional military strength relative to foreseeable potential adversaries, it is likely that future foes will attempt to attack the United State in a more indirect manner by using "asymmetrical warfare." Asymmetrical warfare focuses on defeating the superior with the inferior. Examples include terrorism, informational warfare, and the use of chemical, biological and nuclear (CBR) weapons. Potential asymmetrical attacks to the continental United States pose substantial challenges to the current operational structure from which so much of our military strength is derived. Examined are the elements that effect our preparedness in responding to a domestic asymmetrical attack: The complexities asymmetrical threats present in operational planning; unified command structuring; interagency coordination; and legal jurisdiction. A hypothetical scenario employing Red China's current asymmetrical warfare capabilities is depicted to reinforce the pertinence of the topic. This paper examines the current operational system, issues that inhibit the operational process and offers for consideration areas of potential improvement.

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** C	

CONTENTS

ABSTRACT

The United States position of military dominance has continually evolved since World War II. While many factors are responsible for this elite status, perhaps the most important is the careful consideration given to jointness and operational effectiveness. Given the Unites States' seemingly overwhelming conventional military strength relative to foreseeable potential adversaries, it is likely that future foes will attempt to attack the United State in a more indirect manner by using "asymmetrical warfare." Asymmetrical warfare focuses on defeating the superior with the inferior. Examples include terrorism, informational warfare, and the use of chemical, biological and nuclear (CBR) weapons. Potential asymmetrical attacks to the continental United States pose substantial challenges to the current operational structure from which so much of our military strength is derived. Examined are the elements that effect our preparedness in responding to a domestic asymmetrical attack: The complexities asymmetrical threats present in operational planning; unified command structuring; interagency coordination; and legal jurisdiction. A hypothetical scenario employing Red China's current asymmetrical warfare capabilities is depicted to reinforce the pertinence of the topic. This paper examines the current operational system, issues that inhibit the operational process and offers for consideration areas of potential improvement.

Introduction

> ***"Not only is their equipment better, so too is their logistics system, their organization, their command structure, their leadership and their personnel. The Americans take operations seriously. They have thought through their problems, found solutions and now are the only first-class fighting force in the world."***
>
> **-John Keegan, *Powerful***

Through the "process" of operational art the United States has become the premier military in the world. The complex multi-service and multinational relationships that are a fact of modern conflicts would be unmanageable without the structure provided within the framework of operational art. It is important that the same operational thoroughness that made the United States military conventionally dominant be applied across the entire spectrum of threats that may potential confront the United States in the future. It simply makes sense that areas of responsibility and cognizance of command be well defined and established for all levels of a military action.

Much of what we today refer to as the study of "operational art" comes from the lessons learned from World War II. Since much of what is operational art was empirically derived, voids may exist in areas where little historical experience is available. The same emphasis that has been placed on jointness, command structure, identification of threats, and contingency planning may be severely lacking in homeland defense, especially in the area of asymmetrical warfare. The United States military, both in forces and command structure, is geared toward a conventional foe. This paper addresses the existing operational structure for the continental United States (CONUS) area of responsibility (AOR), and problems caused and shortfalls encountered when dealing with an asymmetrical threat.

Historically, strategic thinkers have viewed asymmetrical threats as isolated instances to be acted on in an ad hoc manner as circumstances arise. The interoperability and jointness

concerns driving operational doctrine evolving from the post World War II era to the present day were focused on inter-service rivalries against a conventional military opponent. As we enter the next millenium this focus must continue to expand and shift to include interagency operability and asymmetrical threats. I will pose several points for consideration, in the framework of operational art, that have far-reaching implications for the conflicts of the future.

Specifically I will address:

1. The operational relevance of the topic
2. The focus of USACOM responsibility (functional v. geographic)
3. Problems of coordinated effort of interagency response
4. The fragility of critical United States infrastructure
5. The legal issues concerning domestic use of the military

Finally, I will describe a hypothetical scenario, based on research of the capabilities of one potential future adversary (Red China), to illustrate both the existing problems and gravity of inadequate or untimely response.

Asymmetrical Threats

It seems likely that for the immediate future, no potential adversary can match the United States military conventional forces in a direct conflict. Having learned the lessons of Iraq's defeat in the 1991 Persian Gulf War, future enemies are unlikely to confront United States military power head-on, since they would be almost certain to lose.[1] Instead future adversaries will likely pursue an indirect or asymmetrical engagement, seeking to counter technological superiority by exploiting the limitations and vulnerabilities of our high-tech weapons. In submissions to the Joint Strategy Review, the Armed Services have emphasized emerging security threats such as terrorism, biological weapons and information warfare. Particularly

vulnerable to these threats are the forces and resources of CONUS. Asymmetrical acts constitute a complete, self-contained military art, separate from the old rules of conventional warfare on which our defense principals are based. As former Senator Sam Nunn observed at a conference on weapons of mass destruction terrorism held last May in Washington, D.C., "The threat over the next decade may come by missile, but it is more likely to arrive by suitcase"[2]

The reality and gravity of this threat is exemplified by the appointment of Gen. Henry Shelton as the Chairmen of the Joint Chiefs of Staff. General Shelton was previously the Commander-in-Chief (CinC) of the United States Special Operations Command (SOCOM). "General Shelton was [William] Cohen's inevitable choice to become the chairmen to lead the military into an era of unconventional futuristic warfare which the Secretary believes is already here."[3] Cohen's view is: "The USA has such overwhelming power that other countries now will, in fact turn to asymmetrical types of threats. [Gen. Shelton] will steer the U.S. military to be much more flexible, more creative, trying to examine ways and anticipate ways in which the adversary will try to exploit our weaknesses."[4]

Unfortunately the top-level view of this threat does not match either the current acquisition strategy or operational structure and focus of our forces. The priorities for modernization continue to focus on costly Cold War weapon systems, which will be ineffective and most susceptible to these threats. "It is one of the curious features of the most modern weapon that it is especially effective against the most modern types of civilizations."[5] The current operational structure of the United States forces contains many flaws, often of simple omission, which may be magnified and exploited by asymmetrical threats.

Functional Focus of USACOM

We have been fortunate in this country that our 20th century wars have been fought on foreign soil. This history, when coupled with our current overwhelming conventional military strength, tends to foster a belief that we are invulnerable. We must not be complacent about such a possibility in future conflicts. Of the eight standing concept plans (CONPLANs) and four function plans within ACOM, none specifically address homeland defense against asymmetrical warfare. On 1 October 1993, the planned consolidation of operational responsibility took a giant step forward with the establishment of Atlantic Command (USCINCACOM), assuming control of FORSCOM, ACC, LANTFLT, and MARLANT. The newly consolidated command became at once both a geographic and functional CINC. In its functional role USACOM's primary mission is to develop mechanisms to ensure commanders, staff and units are properly integrated, trained and ready to meet crisis, contingency, and war time requirements of a supported combatant commander.[6] In the aftermath of the Cold War and subsequent worldwide draw down of American forces, this remains the primary and overwhelmingly important focus of ACOM. The fact remains, however, that ACOM has geographic operational responsibility over the continental United States.

The USACOM mission statement as listed in the ACOM Implementation Plan:

1. Train forces as joint units.
2. Provide joint forces to warfighting CINCs.
3. Execute responsibilities as assigned.

The USACOM implementation plan clearly intimates its functional priority: "As Unites States presence is reduced, combatant commanders will be more dependent on CONUS-based forces to augment overseas missions. These forces must be highly skilled, rapidly deliverable, and fully

capable of operating effectively as a joint team on arrival."[7] The organization of USACOM is set up according to this primary mission: "It is organized to serve as the Joint Force Integrator with the responsibility to conduct joint training of assigned CONUS-based forces and to develop and exercise joint force packages for rapid global deployment to combatant commands for joint or combined operations, as directed."[8] With the emphasis being placed on this new "functional" requirement for USACOM, fewer resources are available to be applied toward identifying and combating future threats within the USACOM AOR. Force planning, or the determination of force requirements, availability, shortfall identification, and resolutions, clearly identifies the principle combat forces required by the concept of operations planned. Without an overall assessment of all capabilities, both within and external to the Defense Department, and the associated command relationships, it is likely that any attempt at force planning for a major asymmetrical threat would be deficient. This responsibility becomes even more difficult when considering the command relationships that are invoked for a military response, particularly to an asymmetrical threat, within the United States. The ability to globally supply well-trained troops and equipment should not eclipse ACOM's geographic responsibilities. Paramount is the need for pre-planning, identification of potential shortfalls, and delegation of authority and responsibility.

Campaign Planning

Perhaps more than anything else, campaign planning embodies the essence of operational art:

> ***"A campaign plan isn't a document that springs into existence only after a war begins; rather, it continues through time as the operational extension of the commander-in-chief's theater strategy for peace and crisis, as well as war. A campaign plan translates strategic guidance into operational direction for subordinates."***
>
> **-Mendel and Banks, *Campaign Planning: Getting it Straight***

The operational level is best summarized as the overall orchestration and control of the various components (tactics) that are used to achieve some strategic goal. In the military this is best characterized in the essence of the campaign plan. United States Army Field Manual 100-5 defines "operational art" as the employment of military forces to attain strategic or operational objectives within a theater through the design, organization, integration and conduct of campaigns, major operations and battles.[9] A campaign is further defined as a series of related military operations designed to achieve strategic objectives within a given time and space. A campaign plan describes how these operations are to be conducted. The Commander in Chief (CinC) of a unified command, e.g. ACOM, has the responsibility for the development of joint operation (campaign) plans. Operational art involves fundamental decisions about where, when and how to fight: A careful consideration of the ends to be achieved, the ways in which to achieve the ends, and how to use the means available. It is important that a clear, understandable and achievable mission statement, defining the desired strategic end-state is provided to the operational commander. Equally important is that the mechanism is in place to insure the proper coordination for the implementation of "all" available functional capabilities (means) available. To this point strategic thinkers have viewed asymmetrical threats as isolated instances to be acted on in an ad hoc manner as circumstances arise. As mentioned above, no standing concept plan or function plan is available to be translated into a campaign plan or OPORD in a crisis situation.

Interagency Coordination

The Joint Chiefs of Staff was created as a recommendation panel from the U.S. President, with the goal of determining correct military response, putting aside inter-branch rivalry and thus presenting the President with a clear, unbiased military option. For a response against an asymmetrical threat to be effective, the military organizational structure must adapt and

incorporate the many vastly differing federal, state and local agencies and departments. These relationships pose a severe organizational obstacle in the campaign plan framework. Has the Department of State developed a complete understanding of the five-paragraph format? How about the New York City Police Department? Without the synergy provided from a common lexicon and procedures, the already arduous task of a coordinated response becomes unworkable.

At the operational level effective response to potential asymmetrical threats depends on the ability to respond quickly and decisively. "A threat can only be neutralized by the rapid application of contingency plans by trained personnel."[10] This requires an effective and cohesive response program that facilitates interagency cooperation between DoD, federal, state and local authorities, and takes advantage of the unique expertise of each and clearly defines lines of responsibility and authority. The complexity of this problem is enormous. For example, in New York City, unless a federal statute has been violated, thereby involving the FBI, the local police are responsible for law enforcement. Even in a federal matter the Federal Aviation Administration and/or the State Department may be responsible rather than the FBI. Plans for emergency readiness are even more chaotic: For example, within the United States 175 interagency committees and groups would be involved in the case of a nuclear terrorist incident.[11]

A prelude to the types of problems caused by multiple agency interoperability is seen in the more and more frequent "Military Operations Other Than War" (MOOTW). The difficulty and enormity of this problem has been exposed recently in Bosnia. Former Chairman of the Joint Chiefs of Staff Gen. John Shalikashvili addressed this issue during a conference on Bosnia held in Brussels in April 1996. He stressed the importance of the Dayton Peace Agreement, which outlines the roles and responsibilities within the strategic framework of the Bosnian

mission. It is clear that interoperability between military and civilian agencies was and is lacking and that this must improve if a more symbiotic relationship is to develop. Until that is accomplished, the military will continue to see its mission in isolation. When asked what he saw as the priorities of the military in assisting the civilian agencies in achieving the overall desired end state, Shalikashvili replied; "I think the priority is first on the military tasks, probably we can contribute the most to the civilian effort if we concentrate in the next phase on widening the climate of overall security."[12] While this may indeed be true, I believe this reveals a lack of unity of effort and interoperability. I believe this exposes our current capacity for protection against asymmetrical attack as a critical vulnerability. For a crisis within the United States these problems would increase by orders of magnitude, as would the consequences of inapt response.

Crisis Response Procedures

The asymmetrical threats described thus far would fall under what the Joint Staff refers to as a domestic crisis situation. A crisis is defined as a situation where important national interests are threatened, response time is short, often little or no warning is available; where the commitment of military forces and resources is contemplated to achieve national objectives. The operational command structure outlined in the Crisis Action Procedures, generated by the J-3 Operations Directorate The Joint Staff, differs from the standard operating procedure. For example, for a crisis within the United States, the Secretary of Defense has tasked the Secretary of the Army as the Director of Military Support (DOMS). In this role he becomes the Executive Agent to plan for and commit resources in response to requests from civilian authorities for military support in domestic operations. As the DOMS, the Secretary of the Army has authority to task the CinC's, Services, and Defense agencies to provide forces; however, the commitment of these forces is coordinated via the Joint Staff.[13] This seems to be an inversion of command

relations as the USACOM normally receives operational direction from the NCA through the CJCS and tasks the Service components to provide designated forces as directed by the Secretary of Defense to operate under the direction of USACOM, e.g. under a Joint Task Force or JTF. When required, the Secretary of the Army will convene a Crisis Response Team (CRT) under DOMS with representation from all services and agencies. The CRT operates from the Army Operations Center in the Pentagon and facilitates rapid decision making when multiple service assets are in use.[14]

The CRT would receive direction from the National Security Council (NSC). The NSC Staff supports the President and senior decision-makers directly in all crises affecting the United States national security interests, and is the lead agency in national domestic crisis response. The operational role and authority of the CRT may be limited. In a recent House testimony on federal capabilities for domestic crisis response, strict emphasis is placed on retaining operational control at the NCA level for any military action within the United States. The President would decide, based on the advice of the Attorney General, and it would be a last resort in extreme cases of highly sophisticated or large-scale paramilitary terrorist operations. Once the decision was made, the President or his designee (the Attorney General or his representative) would establish a specific military objective and the degree of force authorized.[15] Within the assigned mission, the military unit would function under the tactical command of the military commander. The overall operational control of the federal response would be retained by civilian authorities. This clearly goes against the principle of centralized planning /decentralized execution and poses many command relationship problems. These complex organization problems are within the military and don't even begin to address the significantly more complex interagency issues.

United States Infrastructure Vulnerabilities

Thus far I have isolated my discussion of an asymmetrical attack on American soil to the to the issue concerning the implementation and use of military forces, i.e. USCINCACOM. It is likely however that the overall objective of such an attack would be to coerce American will in some other conflict. If this assumption is correct, it implies that the American military would simultaneously be engaged elsewhere in conflict. Much consideration has been given to the difficulties posed by a two MRC response. What if one of the engagement areas is CONUS?

One far-reaching effect to all operational commanders would be the stress placed on the command and control infrastructure that such an attack would cause. This could come in either a direct attack such, e.g. informational warfare, or indirectly through the general hysteria a major asymmetrical attack would cause. Consider the effect of a nuclear, chemical, or biological attack against one or several major urban areas. The potential aftermath could be an America that is ground to a halt by: overloaded communication networks, general mass confusion and disorder of the population, as well as economically crippled by ceasing production capability. The potential exists for such asymmetrical threats to cause massive casualties quickly and overload area and national communication networks and snarl coordination among emergency response teams, generating chaos and hysteria. The effects would not only be devastating domestically, but also to any concurrent regional conflict which would most likely be the cause of an asymmetrical attack against the United States.

President's Commission on Critical Infrastructure Protection (PCCIP)

In response to this concern the President's Commission on Critical Infrastructure Protection has been tasked to bring together the combined forces of government, in conjunction

with the private sector, to develop a strategy and operational plan for assuring the continued operation of this nation's critical infrastructure. These include telecommunications, electric power systems, gas and oil transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue) and continuity of government.[16] The integral role played by the Defense Department is exemplified by the naming of Deputy Secretary of Defense John Hamre as a key member of the five person Executive Steering Committee. The Defense Department will need to work closely with all levels of government as well as key members of the private sector. In accordance with Executive Order 13010, the role and mission of the commission is to:

1. Identify and categorize the range of threats to critical infrastructures.
2. Identify vulnerabilities within and among critical infrastructures.
3. Find and assess options for protecting infrastructures, assuring continuation and restoration of service.
4. Develop a strategy for protection of critical infrastructures.
5. Recommend an implementation plan for protection and assurance measures, including the policy, legislative and other changes required.

A report on the Commission's findings including an implementation plan is due early this year. This important first step could be the vehicle necessary to develop command relationships and could eventually be developed into the framework of a concept plan (CONPLAN)/ base campaign plan that is so lacking in this area.

Legal Implications

The general parameters for a response to a domestic crises are outlined in the 1993 issuance of Joint Publication 3-07.2. The publication develops roles and responsibilities for operational level commanders, emphasizing operational protection. It places the Department of

State as the lead agency for terrorist incidents outside the United States, the Department of Justice for incidents within the United States and the Federal Aviation Administration for an airline related crisis. The United States policy on this form of asymmetrical warfare very clearly states that "All terrorist actions are criminal."[17] This seems at odds with "the National Security Directive orders that constitute a *Declaration of War* against an unspecified terrorist foe, to be fought [with military force] at an unknown place and time with weapons yet to be chosen."[18] This is an extremely important issue for military planners, as public law prohibits the use of the military for law enforcement. (See Posse Comitatus, below)

Joint Publication 3-07.2 makes a valiant attempt at defining the complex criminal jurisdictions of federal, state, and local law enforcement agencies emphasizing the importance of the state or federal interests sought to be protected and the capability and willingness of state or federal authorities to act. This jurisdictional dissection of the differing situations is necessary from a legal viewpoint, but may cause confusion of resource allocation and slow a potential response. The publication does address operational protection, and together with DoD Directive 0-2000.12 outlines the DoD THREATCON system.

Posse Comitatus

The Crisis Action Procedures state "Military Commanders are empowered to provide immediate response to save lives, prevent suffering, and mitigate property damage" in a domestic crisis situation.[19] However; legislative prohibitions to domestic use of the military severely restrict or even contradict this statement. A major hindrance to the operational planning and implementation of a structured coordinated process involving the military to combat potential asymmetrical threats is the existence of the Posse Comitatus Act. The Posse Comitatus Act was passed in the aftermath of the United States Civil War, and its basic intent was to insure

that the military was not used to influence election results or seize control of state legislatures. The act outlaws "willful use of any part of the Army or Air Force to execute the law unless expressly authorized by the Constitution or an Act of Congress."[20] (The language of the law mentions only the Army and Air Force, but is applicable to the Navy and Marines by virtue of administrative action and command of other laws.) Posse Comitatus[21] was characterized in 1949 by Judge Magruder of the First Circuit in Chandler v. United States[22] as "...this obscure and all-but-forgotten statute"[23], but has received a great deal of attention due to a modification enacted in 1981 (10-U.S.C. 371-381) in support of the Reagan Administration's "War" on Drugs. The modification allows for the Department of Defense to provide information, equipment, training, and advice to civilian law enforcement agencies. In the entire 120 year history of the Posse Comitatus Act, not a single person has ever been charged with violating it.[24] The recent court applications of the act were in the area of the admissibility of evidence in drug cases in which the military was actively or passively involved.

The issue of an asymmetrical threat to the United States poses a much broader implication of the Posse Comitatus Act as it exists today. By definition, much if not all of what I have described as the asymmetrical warfare threats against the United States are illegal acts, either explicitly, as in the case of terrorism, or implicitly, and therefore constrained by Posse Comitatus. The existence of such a constraint is a serious impediment to the theater wide processes that are essential to the planning, coordination, conduct and sustenance of the whole range of military operations across the spectrum of homeland defense. How can planners develop an effective campaign plan when very implementation would be illegal?

Red China Threat

Recently, several papers have been published (e.g. Ralph Peters, "After the Revolution"; Charles Dunlap, "How We Lost the High-Tech War of 2007") cautioning against an over-reliance on the Revolution in Military Affairs (RMA) . These authors paint darkly the consequences of potential future conflicts, which may occur with lesser military powers such as Iran, Iraq and Red China. They caution against stripping our post Cold War capabilities and over-reliance on the "high tech" solutions offered by the RMA proponents. It struck me while reviewing these insightful articles that, when considered in perspective of this paper topic, the bleak prospects forecasted may in actuality be much worse if combined with the very real near term threats of an asymmetrical attack against the United States. For illustrative purposes regarding the impact and consequences of my topic, I have researched the capabilities and military focus of one of these potential adversaries: Red China.

As early as 1985 Chinese research began to focus on identifying a list of future United States military vulnerabilities and how to exploit them. Open source Chinese military writing on future warfare, including numerous Chinese books and articles, suggest an active research program has been underway for several years in the asymmetrical arena. They examine how China should develop future military capabilities to defeat the United States by exploiting the Revolution in Military Affairs more effectively and more rapidly than the United States, particularly by tailoring new technology to *defeat the superior with the inferior* with a strategy of *asymmetrical warfare.*[25] The underlying theme of these PLA writings is that in order to be successful, "the requirement for the inferior (PLA) to preemptively strike the superior (U.S.) in order to paralyze its nerve centers and block his logistics."[26] This almost certainly refers to an asymmetrical attack to the United States homeland.

Hypothetical Scenario

Take for instance the case where we are involved in the Pacific with Red China over Taiwan. Now consider the effects that the following sequence of coordinated asymmetrical assaults to the United States would cause:

- Information warfare attacks through computer viruses and "electrical incapacitation systems" *, targeting American electrical power systems, civilian aviation systems, transportation networks, telecommunication systems, computer centers, factories and so forth.

- After an initial informational blow was dealt, follow-up terrorist style attacks on urban law enforcement commands either coordinated with or masked as efforts by transnational drug organizations.

- The detonation of biological agents in the frenzied urban shopping areas of in Los Angeles, Chicago, and Washington, D.C, as the American public instinctively purchases large amount of bread, milk and batteries, its seaming panacea to any crisis.

- A diesel submarine surfaces in New York harbor releasing a UAV with a small nuclear device targeting Manhattan.

All of these are relatively low cost, low risk alternatives to conventional warfare that would cripple the United States both domestically and in the Pacific Theatre. They may seem futuristic or improbable, but they are examples of the exact focus of the Chinese defense program since the early 1980s. The occurrence of any combination of these asymmetrical attacks would have devastating effects.

---

* According to General Sun of the Chinese Academy of Military Science, the above mentioned American equipment and systems are vulnerable to micro scale electromechanical systems that can be controlled with sound. The energy source is a micro-scale microphone that can transform sound into energy. People can use them to infiltrate the enemy's vital equipment and lurk there for as long as several decades. In peacetime, they do not cause any problems. In the event of relations between two countries becoming worse, to the point that they develop into warfare, remote control equipment can be used to activate the system to destroy the enemy's equipment.[27]

Conclusion

> ***"The nature of modern warfare demands that we fight as a joint team. This was important yesterday, it is essential today, and it will be even more important tomorrow. Joint Vision 2010 provides an operational based template for the evolution of the Armed Forces for a challenging and uncertain future. It must become a benchmark for Service and Unified Command vision."***
>
> **-Joint Vision 2010**

So sayeth our conceptual template for the future. It is important for future planners to keep in mind that our joint team includes other members besides the Armed Forces and the uncertain future may include asymmetrical threats to our home soil. In order to meet future challenges presented by asymmetrical threats to the United States, the synergy and jointness that has evolved between the service branches must continue to expand to include agencies outside the defense department. Organizational command and control is the most important operational function. In order that our country's full capabilities and assets may be efficiently brought to bear against a domestic asymmetrical threat, steps should be taken to insure the structure is in place and operable before a crisis arises. This will not only facilitate the response, but also identify areas of deficiency that need to be rectified.

The opportunity exists for foresight in further applying the operational art process to the exigency of asymmetrical warfare attacks against the United States, but this will require taking the next step in interoperability, that being looking outside the Defense Department. I have addressed many reasons why this is an extremely difficult task, but one that is demanded by the catastrophic effects of complacency. Bureaucratic barriers that hinder this process should be torn down. Legal impediments such as the obsolete Posse Comitatus Act should be removed. Interagency roles and responsibilities need to be more clearly defined.

The operational performance displayed in Dessert Shield/Storm was exemplary, but the path to the current standard was not without its bumps. Take for instance the evolution of the

Joint Task Force (JTF) from Dessert I → Urgent Fury → Just Cause → Desert Storm. Can we afford the same learning aches and pains for future responses to asymmetrical warfare attacks to the United States?

NOTES

[1] Jonathan B. Tucker, "Asymmetric Warfare: An Emerging Threat to U.S. Security," *The Quadrennial Defense Review*, May 1997 [journal on-line]; available from http://www.comw.org/adr/tucker.htm; Internet; accessed 29 December 1997.

[2] Ibid.

[3] Janes Information Group Limited 1997, "Editorial," *Janes Defence Community*, 13 August 1997 [journal on-line]; available from http://www.janes.com/defence/interviews/970813.html; Internet; accessed 29 December 1997.

[4]Ibid.

[5]Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore: Johns Hopkins University Press, 1989), available from NWC 2263.

[6] The Secretary of Defense. *US Atlantic Command (USACOM) Implementation Plan (1 October 1993)*, Memorandum for the Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretary of Defense for Policy. Washington, D.C.

[7] Ibid.

[8] Ibid.

[9] Department of the Army. *Field Manual 100-5 (14 June 1993)*, Washington, D.C.

[10] Richard H. Shultz Jr. and Stephen Sloan, eds., *Responding to the Terrorist Threat: Security and Crisis Management* (Elmsford, NY, Pergamon Press, 1980), p. 41-42.

[11] J. Bowyer Bell, *A Time of Terror* (New York: Basic Books, 1978), quoted in Schultz and Sloan, *Responding to the Terrorist Threat*, p. 128-29.

[12] General Shalikashvili, question/ answer session, Press Conference on Bosnia, press conference transcript (23 April 1996, available from http://www.usis.it/wireless/wf960423/960423.htm; Internet; accessed 29 December 1997.

[13] J-3 Operations Directorate The Joint Staff. *Crisis Action Procedures: Tailored Response to Crisis Situations (20 September 1995)*, Washington, D.C.

[14] Ibid.

[15] U.S. Congress. House. Committee on the Judiciary. *Federal Capabilities in Crisis Management and Terrorism*. 97th Cong. 1st Sess., February 1981, 49, quoted in WilliamRegis Farrell, *The U.S. Government Response to Terrorism: In Search of an Effective Strategy* (Boulder, Westview Press, 1982).

[16] President's Commission on Critical Infrastructure Protection. *Mission Objectives (20 March 1997)*, Washington, D.C. Available from http://www.info-sec.com/pccip/web/info.html; Internet; accessed 29 December 1997.

[17] Office of the Chairman, The Joint Chiefs of Staff. *Joint Tacticts, Techniques, and Procedures for Antiterrorism (25 June 1993)*, Joint Pub 3-07.2, Washington, D.C.

[18] Brian Michael Jenkins, "Combatting Terrorism Becomes a War," *Newsday*, 13 May 1984, p. 1.

[19] The Joint Staff, *Crisis Action Procedures.*

[20] Congressional Research Service, *The Posse Comitatus Act & Related Matters: The Use of the Military to Execute Civilian Law*, report prepared by Charles Doyle, 104th Cong., 1st Sess., 12 September 1995. CRS Report for Congress 95-9645, CSR-12.

[21] 10 U.S.C.A. §15 (June 18, 1878). Replaced by 18 U.S.C.A. §1385.

[22] 171 F.2d 921,936 (1st Cir. 1949).

[23] C.I. Meeks, "Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act", *Military Law Review 70* (Fall 1975): 83-136, quoted in Department of the Air Force. Air Force Institute of Technology. *A Historical Analysis of the Posse Comitatis Act and Its Implications for the Future*, report prepared by Paull C. Burnett II. Wright-Patterson AFB Ohio, 9 January 1997, 4.

[24] Ibid., p. 6.

[25] Testimony of Dr. Michael Pillsbury. U.S. Cong. Senate. Select Committee on Intelligence, *Chinese Views of Future Warfare: Implications for the Intelligence Community*. 105th Cong., 1st Sess., 18 September 1997. Reprinted in *Miami Herald*, 20 September 1997, available from http://www.herald.com/extra/archive/chinarep.htm; Internet; accesssed 29 December 1997.

[26] Ibid.

[27] Ibid.

SOURCES CONSULTED

BOOKS AND ARTICLES

Bell, J. Bowyer. *A Time of Terror* (New York: Basic Books, 1978).

Builder, Carl H. *The Masks of War: American Military Styles in Strategy and Analysis Crisis Management* (Elmsford, NY, Pergamon Press, 1980). (Baltimore: Johns Hopkins University Press, 1989). Available from NWC 2263.

Janes Information Group Limited 1997, " ," *Janes Defence Community*, 13 August 1997 [journal on-line]. Available from http://www.janes.com/defence/interviews/970813.html. Internet. Accessed 29 December 1997.

Jenkins, Brian Michael. "Combatting Terrorism Becomes a War." *Newsday.* 13 May 1984.

Meeks, C.I. "Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act." *Military Law Review 70* (Fall 1975).

Shalikashvili, General. Question/ answer session. Press Conference on Bosnia, press conference transcript (23 April 1996). Available from http://www.usis.it/wireless/wf960423/960423.htm. Internet. Accessed 29 December 1997.

Shultz, Richard H. Jr. and Stephen Sloan, eds. *Responding to the Terrorist Threat: Security and*

Tucker, Jonathan B. "Asymmetric Warfare: An Emerging Threat to U.S. Security," *The Quadrennial Defense Review*, May 1997 [journal on-line]. Available from http://www.comw.org/adr/tucker.htm. Internet. Accessed 29 December 1997

GOVERNMENT PUBLICATIONS

Congressional Research Service. *The Posse Comitatus Act & Related Matters: The Use of the Military to Execute Civilian Law.* Report prepared by Charles Doyle. Nth Cong., xnd sess. 12 September 1995. CRS Report for Congress 95-9645.

Department of the Air Force. Air Force Institute of Technology. *A Historical Analysis of the Posse Comitatis Act and Its Implications for the Future.* Report prepared by Paull C. Burnett II. Wright-Patterson AFB Ohio. 9 January 1997.

Department of the Army. *Field Manual 100-5 (14 June 1993)*, Washington, D.C.

J-3 Operations Directorate The Joint Staff. *Crisis Action Procedures: Tailored Response to Crisis Situations (20 September 1995).* Washington, D.C.

Office of the Chairman, The Joint Chiefs of Staff. *Joint Tacticts, Techniques, and Procedures for Antiterrorism (25 June 1993).* Joint Pub 3-07.2. Washington, D.C.

President's Commission on Critical Infrastructure Protection. *Mission Objectives (20 March 1997)*, Washington, D.C. Available from http://www.info-sec.com/pccip/web/info.html. Internet. Accessed 29 December 1997.

The Secretary of Defense. *US Atlantic Command (USACOM) Implementation Plan (1 October 1993)*, Memorandum for the Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretary of Defense for Policy. Washington, D.C.

Testimony of Dr. Michael Pillsbury. U.S. Cong. Senate. Select Committee on Intelligence. *Chinese Views of Future Warfare: Implications for the Intelligence Community*. Nth Cong. xnd sess.18 September 1997. Reprinted in *Miami Herald*, 20 September 1997. Available from http://www.herald.com/extra/archive/chinarep.htm; Internet. Accesssed 29 December 1997.

U.S. Congress. House. Committee on the Judiciary. *Federal Capabilities in Crisis Management and Terrorism*. Th Cong. Xst sess., date, 49, quoted in William Regis Farrell, *The U.S. Government Response to Terrorism: In Search of an Effective Strategy* (Boulder, Westview Press, 1982).